UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,239	01/26/2001	Jeffrey Bruce Lotspiech	ARC920010006US1	6974

7590 05/16/2005

John L. Rogitz
Rogitz & Associates
Suite 3120
750 B Street
San Diego, CA 92101

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/771,239	LOTSPIECH ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *20-27* is/are allowed.

6)☒ Claim(s) *1,3-19 and 28-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A Request for Continued Examination was received on 17 February 2005. No claims have been amended, added, or canceled. Claims 1 and 3-30 are currently pending in the present application.

Response to Amendment

2. The declaration originally filed on 21 September 2004 under 37 CFR 1.131 has been entered as of the RCE filed 17 February 2005. The declaration is sufficient to overcome the Yoshida reference as to all claims except for claims 8-11, 18, 19, and 28, as set forth in the previous Final rejection.

3. It is noted that the declaration is not sufficient to swear behind Schwenk, US Patent 6222923, because the declaration does not establish conception or reduction to practice prior to 15 December 1997, the filing date of Schwenk.

Response to Arguments

4. Applicant's arguments filed 17 February 2005 have been fully considered but they are not persuasive.

Claims 1 and 3 were rejected under 35 U.S.C. 102(e) as anticipated by Schwenk, US Patent 6222923. Claims 8-11, 18, 19, and 28 were rejected under 35 U.S.C. 103(a)

as unpatentable over Schwenk in view of Yoshida et al, "A Subscriber-Excluding and Traitor-Tracing Broadcast Distribution System".

Regarding Claim 1, Applicant asserts that, of the cited portion of Schwenk, column 4, lines 8-33, only lines 13-16 mention forming new subsets. The Examiner disagrees with this assertion; specifically, lines 29-33 disclose determining the intersection of two sets. The intersection of the sets is a subset of each of the two sets, and this subset contains the location of the traitor receiver. Therefore, the Examiner believes that this does indeed correspond to dividing and forming new traitor subsets. Applicant further asserts that Schwenk, at column 4, lines 35-39, suggests multiplying its scheme rather than dividing a subset. This is a spurious argument, as the cited portion is merely a statement that the example used of four customers is strictly non-limiting and that traitors may be found within a larger group.

Regarding Claim 8, Applicant begins by stating, "Claim 8 explicitly states that its elements are a non-limiting way to generate the set of subsets, a limitation not mentioned in the Office Action". However, the Examiner fails to appreciate this argument, as the claim recites, "wherein the set of subsets is generated by" the recited steps of assigning, selecting, partitioning, and encrypting. Further, Applicant argues that Schwenk does not mention a revoked set. However, this phrase only appears in the claim in the limitation "partitioning receivers not in a revoked set R into a set of disjoint subsets". Therefore, the Examiner believes that Schwenk does indeed teach partitioning receivers into a set of disjoint subsets (column 3, lines 36-42). It is clear that no receivers have been revoked at this point of Schwenk's method, so therefore the

receivers that are partitioned are not in a revoked set. Additionally, Applicant argues that the claim also recites encrypting a session key using a set of subset keys. However, the Examiner believes that both of the cited references teach encrypting a session key (see Yoshida, page 249, column 2, lines 11-14, where a session key is encrypted by the encryption algorithm, which also uses information of the subscribers; see also Schwenk, column 3, lines 47-62, and Figure 1, where a session key, namely common key SK, is encrypted with the group keys, which are in turn encrypted with the individual keys).

Regarding Claims 9-11, Applicant argues that Schwenk does not teach the additional features of the dependent claims; however, Applicant's argument fails to comply with the requirements of 37 CFR 1.111(b) because it does not discuss specific differences between the claimed invention and the prior art. The arguments are therefore unpersuasive, and Applicant is directed to the reasons for rejection as detailed below.

The above arguments also apply to the rejections of Claims 18, 19, and 28. Applicant's previous arguments regarding the lack of a suggestion to combine references were addressed in the Final Office action of 24 November 2004, and Applicant has not attempted to rebut that response.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Specification

5. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claim 1 recites the limitation "determining whether the traitor subset represents at least two traitor receivers, and if so, dividing the traitor subset into two child sets". There is no support in the specification for performing such a division based on the determination of whether a subset represents at least two traitor receivers. This is described in further detail below in reference to the rejection under 35 U.S.C. 112, first paragraph.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1 and 3-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Specifically, the language of Claim 1 raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment, or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101. The claim recites the limitation "identifying or disabling the traitor receiver" in the alternative.

Although disabling the traitor would be a clear, useful, and tangible result, it is not clear that identifying a traitor would be a tangible, concrete result in itself. Additionally, it is not clear that the remaining steps of receiving, identifying, and determining are specifically tied to a technological environment, art, or machine. This renders the claims non-statutory. See MPEP § 2106 IV.B.2(b).

Claim 12 is directed to a "computer program device" including a "computer program storage device" that are said to contain a program of computer instructions. However, it is not clear that this "computer program storage device" is explicitly a computer-readable medium. The specification does define a "data storage device with a computer readable medium" (page 7, lines 5-10); however, it is not clear from the claims that the recited limitation of "computer program storage device" corresponds to the "data storage device" of the specification. Therefore, the claims are non-statutory. See MPEP § 2106 IV.B.1(a).

Claim Rejections - 35 USC § 112

8. The rejection of Claims 13, 14, 22, and 23 under 35 U.S.C. 112, first paragraph, is withdrawn in light of the amendments to the claims. The rejection of Claims 1, 3-11, 29, and 30 is maintained as set forth below.

9. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> **The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the**

art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

10. Claims 1, 3-11, 29, and 30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Specifically, Claim 1 recites the limitation "determining whether the traitor subset represents at least two traitor receivers, and if so, dividing the traitor subset into two child sets". There is no support in Applicant's disclosure for performing such a division based on the determination of whether a subset represents at least two traitor receivers. Applicant cites blocks 108 and 112 of Figure 15 as support for the amendments to the claims. The Examiner notes that both in Figure 15 and at page 17, line 15-page 18, line 2 of Applicant's specification, there is support for determining whether the traitor subset contains at least two traitor receiver candidates and dividing the traitor subset based on that determination. It is assumed that it is this latter interpretation which is intended in the claim. Claims 3-11, 29, and 30 are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

12. Claims 1 and 3 are rejected under 35 U.S.C. 102(e) as being anticipated by Schwenk, US Patent 6222923.

In reference to Claims 1 and 3, Schwenk discloses a method including receiving a set of subsets derived from a tree including leaves, each of which represents a receiver (column 3, lines 24-33); identifying a traitor subset as containing at least one traitor receiver (column 4, lines 9-13); and identifying and disabling the traitor receiver (column 4, lines 33-36). Schwenk further discloses dividing the traitor subset into child subsets and removing complementary subsets (column 4, lines 8-33).

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 8-11, 18, 19, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwenk in view of Yoshida et al, "A Subscriber Excluding and Traitor-Tracing Broadcast Distribution System".

In reference to Claim 8, Schwenk discloses everything as applied to Claim 1 above. Schwenk further discloses assigning each receiver private information (column 3, lines 42-51), selecting a session key (column 3, lines 55-62), partitioning receivers not in a revoked set into subsets having subset keys (column 3, lines 36-42), and encrypting the session key with the subset keys (column 3, lines 55-58). However, Schwenk does not explicitly disclose encrypting the false key with the subset keys.

Yoshida discloses a method and system for tracing traitor subscribers in a broadcast distribution system that includes encrypting a false key (page 249, column 2, lines 15-26). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schwenk to include encrypting the false key with the subset key, in order to increase the efficiency of the system with regard to the size of storage and bandwidth required (see Yoshida, page 248, column 1, lines 15-22).

In reference to Claim 9, Schwenk further discloses that the tree includes a root and plural nodes, each node having an associated key (see Figure 1), and that each receiver is assigned keys from nodes in a direct path between the receiver and the root (column 3, lines 42-58).

In reference to Claim 10, Schwenk further discloses that the tree includes a root and plural nodes, each associated with labels (see Figure 1), and that each receiver is assigned labels from nodes above the receiver in the tree, hanging from a direct path between the receiver and the root but not from the direct path (column 3, lines 42-58).

In reference to Claim 11, Schwenk further discloses initializing a cover tree as a spanning tree (column 3, lines 35-47) and iteratively removing nodes from and adding nodes to the cover tree until the cover tree has at most one node (see column 4, lines 8-39).

In reference to Claim 18, Schwenk discloses the following limitations of Claim 12, incorporated in Claim 18 by reference: a computer program device including a means for accessing a tree (column 3, lines 24-33), encrypting a session key (column 3, lines 55-58), identifying a traitor subset (column 4, lines 9-13), and using the traitor subset to identify and disable the traitor device (column 4, lines 33-36). However, Schwenk does not explicitly disclose encrypting a false key.

Yoshida discloses a method and system for tracing traitor subscribers in a broadcast distribution system that includes encrypting a false key (page 249, column 2, lines 15-26). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Schwenk to include encrypting the false key, in order to increase the efficiency of the system with regard to the size of storage and bandwidth required (see Yoshida, page 248, column 1, lines 15-22).

In reference to the limitations of Claim 18, Schwenk further discloses assigning each receiver private information (column 3, lines 42-51), selecting a session key (column 3, lines 55-62), partitioning receivers not in a revoked set into subsets having subset keys (column 3, lines 36-42), and encrypting the session key with the subset

keys (column 3, lines 55-58). Additionally, Yoshida further discloses encrypting a false key (page 249, column 2, lines 15-26).

In reference to Claim 19, Schwenk further discloses that the tree includes a root and plural nodes, each node having an associated key (see Figure 1), and that each receiver is assigned keys from nodes in a direct path between the receiver and the root (column 3, lines 42-58).

In reference to Claim 28, Schwenk discloses the following limitations of Claim 20, incorporated in Claim 28 by reference: a system for determining the identity of a traitor receiver and rendering it useless for decrypting data (column 4, lines 33-36). However, Schwenk does not explicitly disclose using a false key to encode subsets.

Yoshida discloses a method and system for tracing traitor subscribers in a broadcast distribution system that includes encoding subsets with a false key (page 249, column 2, lines 15-26). Yoshida further discloses using the captured pirate receiver for identifying and disabling the traitor receivers (page 249, column 2, lines 32-37). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Schwenk to include encoding subsets with a false key, in order to increase the efficiency of the system with regard to the size of storage and bandwidth required (see Yoshida, page 248, column 1, lines 15-22).

In reference to the limitations of Claim 21, incorporated in Claim 28 by reference, Schwenk further discloses receiving a set of subsets derived from a tree including leaves, each of which represents a receiver (column 3, lines 24-33); identifying a traitor

subset as containing at least one traitor receiver (column 4, lines 9-13); and identifying the traitor receiver (column 4, lines 33-36).

In reference to the limitations of Claim 28, Schwenk further discloses assigning each receiver private information (column 3, lines 42-51), selecting a session key (column 3, lines 55-62), partitioning receivers into subsets having subset keys (column 3, lines 36-42), and encrypting the session key with the subset keys (column 3, lines 55-58). Schwenk additionally discloses that the tree includes a root and plural nodes, each associated with labels (see Figure 1), and that each receiver is assigned labels from nodes above the receiver in the tree, hanging from a direct path between the receiver and the root but not from the direct path (column 3, lines 42-58). Additionally, Yoshida further discloses encrypting a false key (page 249, column 2, lines 15-26).

Allowable Subject Matter

15. Claims 20-27 are allowed.

16. Claims 12-17 would be allowable if the rejections under 35 U.S.C. 101 were overcome.

17. The following is an examiner's statement of reasons for allowance:

Independent Claims 12 and 20 are directed to software implementations of a method for disabling traitor receivers in a broadcast system. The closest prior art, Schwenk, also discloses a method for disabling dishonest receivers. Schwenk specifically teaches the limitations of Claim 12 including a means for accessing a tree,

encrypting a session key, identifying a traitor subset, and using the traitor subset to identify and disable the traitor device. Schwenk teaches similar limitations of Claims 20 and 21. However, Schwenk does not explicitly teach or suggest encrypting a false key. Therefore, the claims are allowable over the cited prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

zad

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER